UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/797,767	03/10/2004	Patrick J. Helland	13768.1423	4181

47973 7590 01/21/2010

WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CTY, UT 84111

EXAMINER	
MORAN, RANDAL D	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
01/21/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/797,767	HELLAND ET AL.	
	Examiner	Art Unit	
	RANDAL D. MORAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 August 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-11,14-16 and 18-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-11,14-16 and 18-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-2, 5-11, and 14-16, and 18-28 are pending in the application.

Below, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-2, 5, 9-11, 13-15, 16, 18-20, 26, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stallings, William. *Cryptography and Network Security; Third Edition.* Chapter 9 / Public-Key Cryptography: 9.1: Principles of Public-Key Cryptosystems. Upper Saddle River, NJ. Prentice Hall, 2003. Pgs. 259-**

265, 290-293, 444, and 655. Hereafter "Stallings" in view of **Bentley et al. (US 2003/0217275),** hereafter "Bentley."

Considering **Claim 1,** Stallings discloses a message encryption system (p.260- lines 28-36, p. 265- Figure 9.4) comprising: a binding component that creates a remote service binding between a user's digital certificate and a remote service associated with a target system(p. 264- lines 18-23, p. 265- lines 1-17, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message), the remote service binding specifying that the user's digital certificate is to be used when a dialog is initiated between the initiator system and the remote service; a session key generator that generates a session key for a dialog between the initiator system and the remote service at the target system, the session key employed to securely exchange a message associated with a dialog (p. 265- lines 18-19); and, an encryption component that employs asymmetric encryption to encrypt the session key using a private key associated with the initiator system to yield a first session key encryption, encrypt the first session key encryption using the public key specified by the remote service binding to yield an encrypted session key output, and securely transmit the encrypted session key output to the target system(p. 292- lines 23-27, p. 293- lines 1-11, Fig. 10.6- (4)), the session key thereafter being employed to encrypt the message and securely exchange the message between the initiator system and the target system (p. 444- lines 19-21, p.655- line 21) , the encryption component

encrypts the message using the session key to yield a first message encryption, and subsequently encrypts the first message encryption using the private key associated with the initiator system to yield an encrypted message output (p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message).

Stallings does not explicitly disclose specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed.

Bentley discloses specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed ([0090]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Stallings by specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed as taught by Bentley for the benefit of streamlining the process of creating signatures and improving quality control (Bentley [0090]).

Considering **Claim 14,** the combination discloses a message decryption system (p. 260- lines 25-36, p. 265- Fig. 9.4) comprising: a session key employed to securely exchange a message associated with a dialog between an initiator system and a remote service running on a target system (p. 264- lines 18-23, p. 265- lines 1-17, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message), the session key twice encrypted using a private key associated with the initiator system and a public key specified according to a remote service binding that associates the public key with the remote service running on the target system; (p. 265- lines 18-19); and, a decryption component that receives the encrypted version of the session key from the initiator system, employs asymmetric decryption to decrypt the encrypted session key using a private key associated with the target system to yield a first session key decryption, and decrypts the first session key decryption using a public key associated with the initiator system to yield the session key (p. 292- lines 23-27, p. 293- lines 1-11), the session key thereafter being employed to decrypt a received encoded version of the message (p. 444- lines 19-21, p. 655- lines 21), wherein the decryption component decrypts the encoded version of the message using the session key to yield a first message decryption, and subsequently decrypts the first message decryption using the public key associated with the initiator system to yield the message (p. 264- lines 18-23, p. 265- lines 1-17, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the

remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message).

Stallings does not explicitly disclose specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed.

Bentley discloses specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed ([0090]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Stallings by specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed as taught by Bentley for the benefit of streamlining the process of creating signatures and improving quality control (Bentley [0090]).

Considering **Claims 18 and 21,** the combination discloses a method facilitating session key encryption comprising (p. 444- lines 19-21): employing a processor executing computer- executable instructions stored on a computer-readable storage medium to implement the following acts: establishing a remote service binding at a first system that binds a service running on a second system with a

particular user's digital certificate (p. 264- lines 18-23, p. 265- lines 1-17, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message); initiating a dialog at the first system with the service running on the second system: identifying the digital certificate bound to the service upon initiating the dialog; firstly encrypting a symmetric session key with a private key associated with an initiator of the dialog to yield a first encryption (p. 264- lines 18-23); secondly encrypting a result of the first encryption with a public key associated with the identified digital certificate to yield a second encryption (p. 264- lines 18-23, p. 265- lines 1-2); and, transmitting a result of the first encryption from the first system to the second system; and employing the session key to encrypt and decrypt messages between the first system and the second system that access the service running on the second system (p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message).

Stallings does not explicitly disclose specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed.

Bentley discloses specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed ([0090]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Stallings by specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed as taught by Bentley for the benefit of streamlining the process of creating signatures and improving quality control (Bentley [0090]).

Considering **Claim 26,** the combination discloses a computer readable medium encoded with a data structure that facilitates secure distributed communication, the data packet comprising: a first data field comprising a remote service binding that associates a service running on a remote system with a particular user's public key (p. 264- lines 18-23, p. 265- lines 1-17, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message); and a data field comprising an encrypted session key, the session key encrypted using a private key associated with an initiator of a message to the service and the public key associated with the service by the remote service binding; a data field comprising an encrypted message, the encrypted message first encrypted with the

session key (p. 265- Fig. 9.4), then encrypted with the private key associated with the initiator of the message (p. 265 - lines 15-17), the message comprising a digital certificate (Bentley [0090]) that is employed as part of a broker service security system that facilitates location transparency of the services (p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message).

Stallings does not explicitly disclose specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed.

Bentley discloses specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed ([0090]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Stallings by specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed as taught by Bentley for the benefit of streamlining the process of creating signatures and improving quality control (Bentley [0090]).

Considering **Claim 27,** the combination discloses a message decryption system (p. 260- lines 25-36, p. 265- Fig. 9.4) comprising: means for creating a remote service binding that associates a service running on a first system with a particular public key; means for initiating a message exchange between the first system and a second system, the message exchange involving access to the service running on the first system (p. 264- lines 18-23, p. 265- lines 1-17, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message); means for receiving an encrypted session key from the second system, the encrypted session key encrypted using a private key associated with the second system and the public key associated with the service by the remote service binding; (p. 264- lines 18-23, Fig. 9.4- item Z); means for decrypting the encrypted session key using a private key associated with the first system to yield a first decryption (p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4); means for decrypting the first decryption with a public key associated with the second system to yield a second decryption (p. 265- Fig. 9.4); means for securely storing a result of the second decryption as a session key (p. 292- lines 23-27, p. 293- lines 1-11, Fig. 10.6- (4)); and, means for employing the session key to decrypt an encrypted message received by the second system (p. p. 444- lines 19-21, p. 655- line 21) , the encrypted message encrypted using the session key and a private key securely associated with the second system (p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4- item Z, according the instant

specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message).

Stallings does not explicitly disclose specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed.

Bentley discloses specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed ([0090]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Stallings by specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed as taught by Bentley for the benefit of streamlining the process of creating signatures and improving quality control (Bentley [0090]).

Considering **Claim 2,** Stallings discloses the session key comprising a 128-bit randomly generated symmetric key (Stallings p. 444- lines 19-30).

Considering **Claim 11,** Stallings discloses (p. 264- lines 18-23) (p. 264- lines 18-23, p. 265- lines 1-2, p. 265- Fig. 9.4) the encryption component separately encrypts the

session key with a public key associated with the target system (p. 260- lines 28-28, p. 261- Fig. 9.1) the separate encryption is provided as an output to the target system together with the encrypted session key output (Fig. 9.1, Fig. 9.4).

Considering **Claim 13,** Stallings discloses a broker security system employing the session key of claim 1 (Stallings p.260- lines 28-36, p. 265- Figure 9.4).

Considering **Claims 5 and 20,** the combination discloses the remote service binding created at the initiator system using the following syntax:

Create Remote Service Binding <LOGICAL SERVICE NAME>

To Service '<SERVICE>'

With (User = [<USER>])

where <LOGICAL SERVICE NAME> is a logical name assigned to the service by the binding, <SERVICE> is the remote service, and <USER> is an identification of the user whose public key is to be utilized when a dialog is initiated with the remote service by the initiator system (Stallings p. 265- Fig. 9.4, Bentley- [0090]).

Furthermore, the examiner points out that the differences (code syntax) between the pending application and the combination is only found in the non-functional descriptive material and are not functionally involved in the steps as currently recited in the claims. The operation of the combination would be performed the same regardless whether the data included the same code syntax. Thus, this descriptive material will not distinguish the claimed invention from the prior art in terms of patentability, see In re Gulack, 703 F.2d 1381, 1385, 217 USPQ 401,404 (Fed. Cir. 1983); In re Lowry, 32 F.3d 1579, 32 USPQ2d 1031 (Fed. Cir. 1994).

Considering **Claim 9,** the combination discloses the public key being stored as a digital certificate (Stallings p. 260- lines 30-32, p. 261- Fig. 9.1- Bob's Public Key Ring).

Considering **Claim 10,** the combination discloses the digital certificate being associated with a user via a login protocol (Stallings p. 290, p. 291- lines 1-11).

Considering **Claim 15,** the combination discloses the message comprising a digital certificate employed as part of a broker service security system (Stallings p. 264- lines 18-23, p. 265- lines 1-19, Fig. 9.4).

Considering **Claim 16,** Stallings discloses the private key being securely associated with the target system (Stallings p. 265- Fig. 9.4).

Considering **Claim 19,** the combination discloses encrypting a message at the first system using the session key to yield a first message encryption, and encrypting the first message encryption at the first system using the private key associated with the identified digital certificate to yield a twice- encrypted message (Stallings p. 265- Fig. 9.4).

3. **Claims 6-8** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stallings and Bentley** in view of **VanHeyningen et al. (US 2002/0112152),** hereafter "VanHeyningen".

Considering **Claim 6,** Stallings and Bentley does not explicitly disclose a plurality of trusted agents that act as a proxy for a publisher to respectively exchange the message with respective subscribers, the trusted agents employing the private key.

VanHeyningen discloses a plurality of trusted agents that act as a proxy for a publisher to respectively exchange the message with respective subscribers ([0092] lines 1-10, [0139] lines 1-8, Fig. 7B), the trusted agents employing the private key ([0039], [0095]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination by a plurality of trusted agents that act as a proxy for a publisher to respectively exchange the message with respective subscribers, the trusted agents employing the private key as taught by VanHeyningen in order to avoid individually delivering messages to each appropriate recipient device in the network (e.g. point-to-point messaging), as this type of communication restricts the speed and efficiency of the invention (VanHeyningen- [0139] lines 1-8).

Considering **Claim 7,** the combination discloses a trusted agent negotiates a unique session key with a subscriber (VanHeyningen- [0039], [0095]).

Considering **Claim 8,** the combination discloses the trusted agents acting in concert to dynamically load balance distribution for the publisher VanHeyningen ([0091] lines 7-12, Fig. 7B- item 704).

4. **Claim 28** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Stallings and Bentley** in view of **Wasilewski et al. (US 5,870,474),** hereafter "Wasilewski".

Considering **Claim 28,** Stallings and Bentley does not explicitly disclose comprising multiple instances of the broker service sharing the same private key such that the application accessing the remote service treats the multiple instances collectively as a unit.

Wasilewski discloses comprising multiple instances of the broker service sharing the same private key such that the application accessing the remote service treats the multiple instances collectively as a unit (column 22- lines 13-34).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination by deploying multiple instances of the service providers sharing the same private key to provide a system where the STU's (targets) would be unable to distinguish between service providers (initiators) (Wasilewski- column 22- lines 13-34).

5. **Claims 22-25** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stallings, Bentley** and **VanHeyningen** in view of **Wasilewski.**

Considering **Claims 22 and 25,** the combination discloses a method facilitating session key decryption comprising (p. 265- lines 18-19, p. 444- lines 19-21): employing a processor executing computer-executable instructions stored on a computer-readable storage medium to implement the following acts: establishing a dialog between a dialog initiator and a service running on a target system(p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4- item Z) receiving at the target system an encrypted session key from the dialog initiator, the encrypted session key encrypted using a private key associated with the dialog initiator and a public key specified by a remote service binding that associates the public key with the service running on the target system (p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. In

Fig. 9.4, the public key of the target is further used to encrypt the message; decrypting the encrypted session key with a private key associated with the target system to yield a first decryption (p. 264- lines 18-23, p. 265- lines 1-2); decrypting the first decryption with a public key associated with the dialog initiator to yield the decrypted session key (p. 265- Fig. 9.4); employing the decrypted session key together with the public key associated with the dialog initiator (p. 265- lines 5-19) to decrypt a subsequent twice-encrypted message from the dialog initiator (Fig. 9.4), and negotiating a unique session key with each of a subscriber accessing one of the multiple instances of the service broker (VanHeyningen- [0039], [0095]).

The combination does not explicitly disclose deploying multiple instances of a service broker that serve to establish dialogs between subscribers and the dialog initiator; sharing the private key associated with the dialog initiator with the multiple instances of the service broker.

Wasilewski discloses deploying multiple instances of a service broker that serve to establish dialogs between subscribers and the dialog initiator; sharing the private key associated with the dialog initiator with the multiple instances of the service broker (column 22- lines 13-34).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination by deploying multiple instances of the service providers sharing the same private key to provide a system where the STU's (targets) would be unable to distinguish between service providers (initiators) (Wasilewski- column 22- lines 13-34).

Stallings does not explicitly disclose specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed.

Bentley discloses specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed ([0090]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Stallings by specifying the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed as taught by Bentley for the benefit of streamlining the process of creating signatures and improving quality control (Bentley [0090]).

Considering **Claim 23,** the combination discloses the private key being securely associated with a target of the message (Stallings- p. 265- Fig. 9.4).

Considering **Claim 24,** the combination discloses the public key being associated with an initiator of the message (Stallings- p. 265- Fig. 9.4).

Response to Arguments

Applicant's arguments with respect to the independent claims have been considered but are moot in view of the new ground(s) of rejection.

Regarding **Claims 1, 14, 18, 22, 26, and 27,** applicant's arguments have been fully considered but are not persuasive.

With respect to applicant's argument that Stallings fails to teach *a binding component that creates a remote service binding between a user's digital certificate and a remote service associated with a target system… the remote service binding specifying that the user's digital certificate is to be used when a dialog is initiated between the initiator system and the remote service*, applicant is directed to Stallings - p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4- item Z. According to the instant specification, [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. Stallings - Fig. 9.4 discloses the public key of the target is further used to encrypt the message. The creation of a remote service binding includes the creation of a secure session between two systems. Stallings discloses the creation of a secure session to allow two systems to communicate securely as described in the claims.

From the examiner point of view the cited reference clearly teaches the creation of a remote service binding between a user's digital certificate and a remote service associated with the target system. The argued term *remote service binding* must be clearly defined in the claimed language, if applicant believes it differs from the cited one. Applicant is reminded that additional modification to clarify the claimed language is necessary for further consideration and distinction from the prior art.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/R. D. M./
Examiner, Art Unit 2435

/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2435